#2

Europäisches Patentamt | European Patent Office | Office européen des brevets

CERTIFIED COPY OF PRIORITY DOCUMENT

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr.	Patent application No.	Demande de brevet n°
	00117995.1	

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 22/02/01
LA HAYE, LE

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 00117995.1

Anmeldetag:
Date of filing:
Date de dépôt: 22/08/00

Anmelder:
Applicant(s):
Demandeur(s):
International Business Machines Corporation
Armonk, NY 10504
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Secure usage of digital certificates and related keys on a security token

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat:	Tag:	Aktenzeichen:
State:	Date:	File no.
Pays:	Date:	Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/[redacted]
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

D E S C R I P T I O N

Secure usage of digital certificates and related keys on a security token

Technical field

The present invention relates to a security token and method for secure usage of digital certificates and related keys on a security token, and more particularly, a secure import of certificates into a security token and their secure usage by applications.

Background of the invention

If a customer orders some goods or services, he often has to sign a contract on paper to testify that he placed the order and is liable to pay for it. If the customer makes the deal over the network instead, he needs the electronic equivalent of signing a paper: digital signature. Such a digital signature must guarantee that a customer cannot repudiate his order.

The different methods for digital signature are based on a asymmetrical key pair. The signing person has a private key which cannot be accessed or used by anybody else. A second key, which is associated to the private key, is known to the public. This key is called public key. Only the unique owner of the private key can sign an order, while everybody can check the signature using the corresponding public key.

The public key is distributed in a certificate, which contains owner's name and public key and some further information. In addition, the certificate has an expiration date. It raises the question how we know that the public key in the certificate is not manipulated? A thrusted authority digitally signed the certificate. To check the certificate signature the public key of the signer is needed, which is in the certificate

of the signer. This certificate is signed by a thrusted authority. The recursion can go on until we arrive at the „root certificate", which is something that we thrust because it was distributed through a trusted channel, like for example shipped with the web server.

The most secure place to store such a private key is a „security token". A security token is a data processing system portable and usable in connection with another data processing sytem or integrated into another data processing system comprising at least a RAM, a ROM, a EEPROM and a microprocessor and specialized functions for accomplishing secure crytographical methods. A smartcard can be considered as the most convenient and most portable security token. Modern smart cards are able to perform the signing operation inside the card. At the same time they do not provide any function to export the private key to the outside.

During the import of certificates to a security token (e.g smart card) the validity of a certificate cannot be checked on the security token. This may create errors during the storage of the certificate objects and afterwards during the usage of such erroneous certificate stored on the token. The usage of key and certificate objects stored in the token cannot be guarantied without valid „root certificate" of the certification authority (CA) which generated the user certificate. The root certificate may only be retrieved from an external database. For example, the user has to search and to retrieve the correct root certificate from an externally available central trusted LDAP directory and after verification of this certificate extract the public key of the root certificate which is very time consuming.

Furthermore, the external database will prohibit the secure use of the related keys stored on the token for off-line operations.

The user certificate will not be securely stored on a token and thus cannot be trusted by applications using token for signature

generation and verification. The validity of certificates stored on token cannot be verified completely off-line.

US Patent 5680458 deals with a method of replacing a private root key when the root private key has been compromised and the recipient of a signed document can no longer be sure that the document was signed by the certifying authority and not by a party which compromised the private key. There is no teaching or suggestion in this patent how a user certificate may be securely stored, used or replaced by security tokens.

It is therefore object of the present invention to provide improved protection of digital certificates and related keys on a security token.

It is further object of the present invention to provide a secure import of user certificates into a security token.

Finally, it is further object of the present invention to provide a secure verification of the user certificate stored on a token.

These objects are solved by the features of the independent claims.

Preferred embodiments of the present invention are laid down in the dependent claims.

Summary of the invention

The present invention relates to a system and method for secure usage of digital certificates and related keys on a security token, and more particularly, a secure import of certificates into a security token and their secure usage by applications.

The root certificate of the certification authority(CA) is used during the initialization of the security token in a secure

environment to transfer the certified public root key of the CA and its attributes into the data structure of the security token. The public rootkey is being write protected. Furthermore, a verification component preferably part of the operating system of the security token will accept afterwards, in a case the certificate has to be replaced, only user certificates having a valid digital signature by the private root key of the CA.

Any application using the user certificates and its related user private keys on the token is able to verify the user certificate using this secure public root key of the CA stored on the token. Preferably, the verification of the user certificate is then even possible during the off-line operation by using the extracted trusted public key of the CA stored on the token.

The present invention will be described in more detail using preferred embodiments with Figures, where

FIG. 1 shows structure and components of a smart card which may be used as a security token

FIG. 2 shows the content of the EEPROM after initialization of the smartcard according to the present invention

FIG. 3 shows a flow chart for verification of a new user certificate on the smart card according to the present invention

FIG. 4 shows a flow chart for creating a signature using the present invention.

A security token may be used in connection with any portable data processing device, e.g personal digital assistant or mobile phone. The present invention will be described in detail on a smart card which may be used a preferred embodiment.

The chip(10) of the smart card (FIG. 1)used by the present invention consists of a microprocessor(12), ROM(Read Only Memory;

18), EEPROM(Electrical Erasable Programmable Read Only Memory;16) and RAM(Random Access Memory;14). Today, most smartcards have an 8-bit microprocessor and in the high end cards there are 16- bit or 32-bit processor available.

An cryptographical processor as used by the present invention is needed for performing signature operations on the card itself. The user's private key never needs to leave the smart card.

The information stored in the ROM(18) is written during chip manufacturing. It contains the operating system and security algorithms (e.g. DES, RSA).

The EEPROM(16) is used for permanent storage of data and is used as storage of user certificates, public key of the CA and root certificate of the CA as well as rootines for accomplishing the present invention,e.g verification of user certificates. This information will be written into the EEPROM(16) during initialization of the smart card preferably.
The RAM(14) is the transient memory of the smart card and keeps the data only as long as the card is powered.

FIG. 2 shows the content of an EEPROM (1) of a smart card necessary to carry out the present invention. At manufacturing time especially during personalisation or initialization of the smart card, the „root certificate(2) of the certificate authority (CA)" and the „public root key(4)" of the CA extracted from the root certificate(2) are securely stored as objects in the EEPROM(1). Both objects(2,4) are stored via an access condition so that they cannot be replaced or deleted by unauthorized operations after the smart card has been issued. The validity dates contained in the root certificat(2) are used to limit the usage of the smart card and the user's key and certificates. There may be several key pairs and related certificates of one or many user stored on the smart card. The maximum number of key pairs(n) to be stored in the EEPROM(1) are defined during creation (e.g personalisation) of the smart card.

The object „user public key (8)" may be stored additionally in the EEPROM of the smart card allowing applications to obtain the public keys of the user faster instead extracting them from the user certificates. This applies accordingly for the „public root key (4)" which may be stored additionally in the smart card.

FIG. 3 shows the single steps of the verification rootine which may be part of the smart card's operating system or may be a separate component called by the operating system or other functions.

A new user key pair (e.g RSA public and private key) may be securely generated on the smart card. When the certificate is requested at the CA by the user for one of his public key this well done together with the „Root Certificate of the CA" stored on the smart card. After the CA has tested the information provided by the user and the root certificate of the CA, the CA generates a new user certificate for new public key.

The new user certificate is returned by the CA to the user's client system and is then stored on the smart card. The smart card operating system validates this new user certificate by checking the digital signature using the stored „public root key of CA" and the signature algorithm (e.g RSA, ECC, DSA). When the signature is valid, the new user certificate is valid.

The verification routine is called every time a new certificate object has to be stored on the card, especially during the initialization/personalisation of the smart card with the user's certificates at card issuing time or during the storage of a replacement certificate at the user's or administrator's client system when e.g the original user certificate expired. A new user certificate is only accepted by the smart card when the digital signature of the certificate provided with the certificate is successfully verified on the card using the public root key of the CA.

The verification routine comprises as least following steps:

1. Sending new certificate from the CA to a data processing system which communicates via a wired or wireless connection with a security token, e.g smartcard via(30)

2. Checking the availability of a public root key in the EEPROM of the smart card(40)

3. Storing the new certificate as temporary object in the EEPROM of the smart card if a public root key is available(50)

4. Generating HASH over the new user certificate temporary stored in the smartcard (50)

5. Verifying digital signature contained in the new user certificate and using „public root key" stored in EEPROM for decrypting digital signature(50)

6. Compare the HASH generated by step 4 with the HASH generated by step 5 if both identical then the new certificate is authenticated (60)

7. Creating a new user certificate object on the smart card and deleting or validating temporary user certificate (80)

8. Optionally, for improving the linking of user public key, user private key, user certificate for public key
these three objects are available as a group with same ID via the application interface for creating and verification of digital signatures.

The new user certificate consists of two parts. The first part, for example, contains data elements relating to the key, the issuer of the certificate, the user, the signature algorithm, the serial number, etc. The second part of the certificate contains a digital signature relating to the first part of the certificate.

A digital signature basically establishes the authenticity of electronically transmitted messages or electronic documents. The process of generating a digital signature can be presented as follows.

From the first part of the certificate a HASH algorithm(e.g.SHA-1, MD5) is used to form a HASH value.

The HASH algorithm compresses the data of the first part of the certificate.

Then the HASH value is decrypted with a crypto algorithm. Decryption is based on the private key of a key pair. In the present case the new certificate is encrypted with private key of the CA.

FIG. 4 shows the communication between smart card and an application installed on a data processing using the present invention.

At a first time a communication is established between an application running on a data processing system and a smart card, the verification routine verifies the availability of CA Root Certificate of a CA on the smart card (110). Then, application obtains the certificate from the smart card, verifies the standard information stored in the certificate (e.g expiration date), retrieves the public root key from the certificate (110) and gets selected user certificate from the smart card which will be used for creating a digital signature. Before that user certificate may be used, the verification routine verifies the digital signature contained in that user certificate, generates a HASH using HASH algorithm specified in the user certificate and uses the „public root key" for decrypting digital signature attached to the user certificate. If both HASHS are identical the user certificate is authenticated (130).

Finally, a HASH is generated over the message to be signed, the

HASH is encrypted with private key and signature algorithm specified in the user certificate resulting in a digital signature (150). The digital signature is attached to the message to be sent(170). A correctly signed message has been generated with the correct user certificate, which proves the validity and the authenticity of the message when received via insecure network(180).

The present invention can also be embedded in a computer program product, which comprises all the features enabling the implementation of the methods described herein, and which - when loaded in a computer system - is able to carry out these methods.

C L A I M S

1. Security Token comprising:

Random Access Memory (RAM 14),

Electrical Erasable Programmable Read Only Memory (EPROM 16)

Microprocessor (12),

Read Only Memory (18),

characterized in that

said EEPROM having at least an object containing a user certificate(6) and an object containing a certificate of the certification authority (CA) of said user certificate (root certificate; 2), wherein said root certificate (2) is being write protected, and a Verification component for checking authentication of said user certificate using information of said root certificate.

2. Security Token according to claim 1, wherein said user certificate (6) comprises at least following information:

Name of issuer
Issuer's ID
User ID
HASH algorithm
Signature Algorithm
Public key
Digital Signature

3. Security Token according to claim 1, wherein said root certificate (2) comprises at least following information:

Certification authority's name

Certification authority's ID
HASH algorithm
Signature Algorithm
Public root key
Digital signature

4. Security Token according to claim 1 comprising the following further objects in said EEPROM:

a) public root key(4)
b) user's public key(8)
c) user's private key (8)

5. Security Token according to claim 1, wherein said Verification component is part of the operating system of said security token.

6. Seurity Token according to claim 1, wherein said Security Token is a smart card.

7. Method for initializing a Security Token comprising the following steps:

a) transferring the root certificate of the certification authority into said security token using a secure transmission environment
b) securing the root certificate against modifications
c) storing a verification component into said security token allowing use or replacement of user certificates only when said user certificate is authenticated by said root certificate.

8. Method according to claim 7, further comprising:

d) storing public root key additionally to said root certificate

9. Method for authenticating information generated by an

application using a Security Token according to claim 1 comprising the steps of:

a) retrieving the public root key from said root certificate (110)
b) generating a HASH over user certificate using HASH algorithm specified in said user certificate (130)
c) retrieving and decrypting the digital signature contained in said user certificate by applying said public root key resulting in a HASH of said user certificate (130)
d) allowing use of said user certificate for signing said information with a digital signature when both HASHs are identical.

10. Method according to claim 9, wherein said information is a document or a mail.

11. Method according to claim 9, wherein said user certificate and said root certificate are sent to said application system and said steps a)-d) are accomplished on said application system.

12. Method according to claim 9, further comprising the step of:

checking the validity of the root certificate before retrieving said public root key.

13. Method for replacing a user certificate stored in a Security Token according to claim 1 comprising the steps of:

a) receiving a new user certificate from the certification authority and storing it into said EEPROM of said security token as temporary object (30;40)
b) generating a HASH over new user certificate using HASH algorithm specified in said new user certificate (50)
c) retrieving said digital signature contained in said new user certificate and decrypting said digital signature by applying said public root key retrieved from said root

certificate resulting in a HASH of said user certificate (50)

d) permanently storing said new user certificate when both HASHs are identical (60; 80)

14. Client-Server system having a client with a Security Token according to claim 1 to 6.

15. Data processing system using a Security Token according to claim 1 to 6.

16. Computer program product stored on a computer-readable media containing software for performing of the method according to 7 to 8, 9 to 12 and 13 if said program product is executed on a computer.

DE9-2000-0056

EPO - Munich
66
22. Aug. 2000

A B S T R A C T

The present invention relates to a security token and method for secure usage of digital certificates and related keys on a security token, and more particularly, a secure import of certificates into a security token and their secure usage by applications.

The root certificate of the certification authority(CA) is used during the initialization of the security token in a secure environment to transfer the certified root public key of the CA and its attributes into the data structure of the security token. The public root key is being write protected. Furthermore, a verification component preferably part of the operating system of the security token will accept afterwards, in a case the certificate has to be replaced, only user certificates having a valid digital signature by the private root key of the CA.

Any application using the user certificates and its related user private keys on the token is able to verify the user certificate using this secure root public key of the CA stored on the token. Preferably, the verification of the user certificate is then even possible during the off-line operation by using the extracted trusted public key of the CA stored on the token. (FIG.3)

THIS PAGE BLANK (USPTO

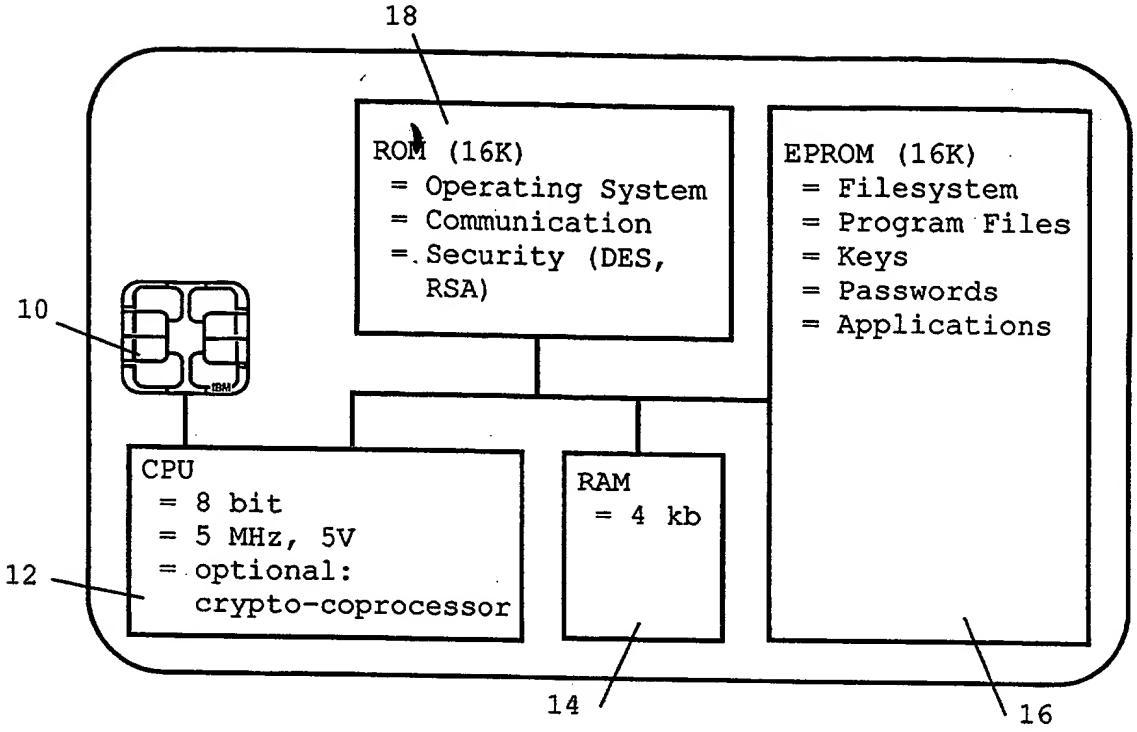

FIG. 1

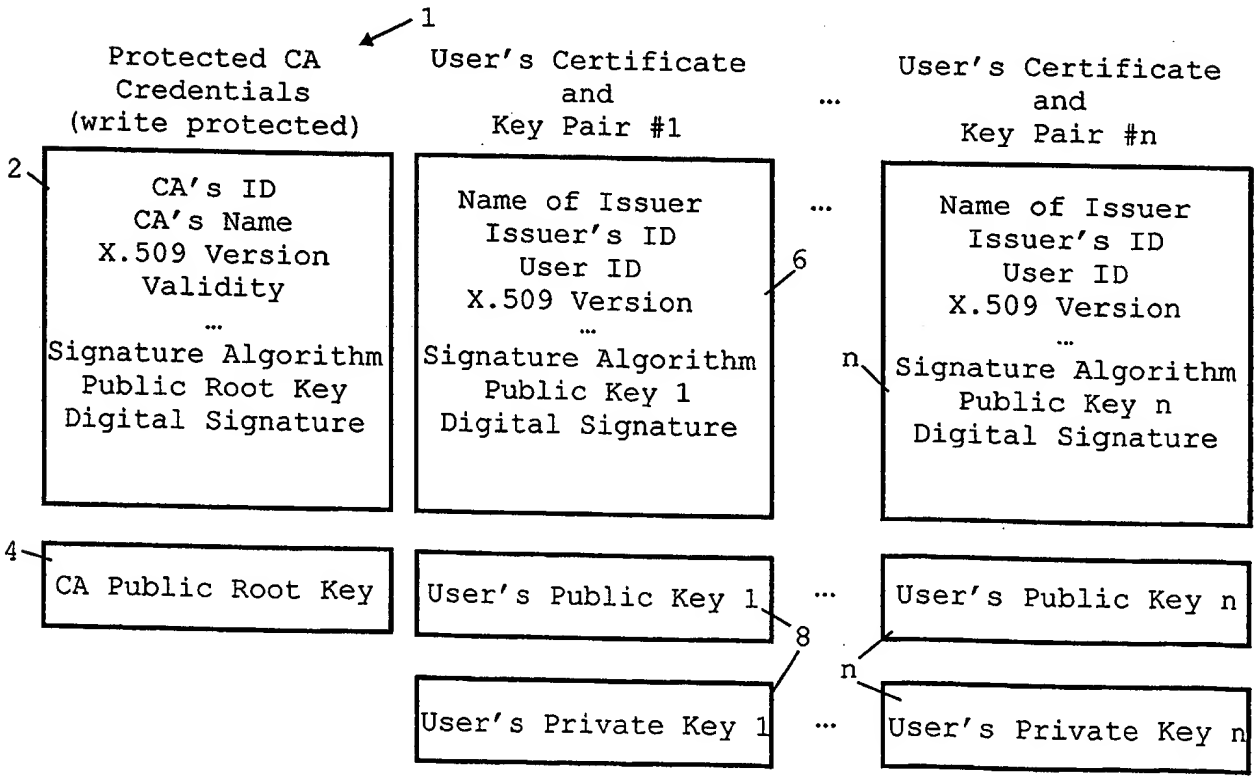

FIG. 2

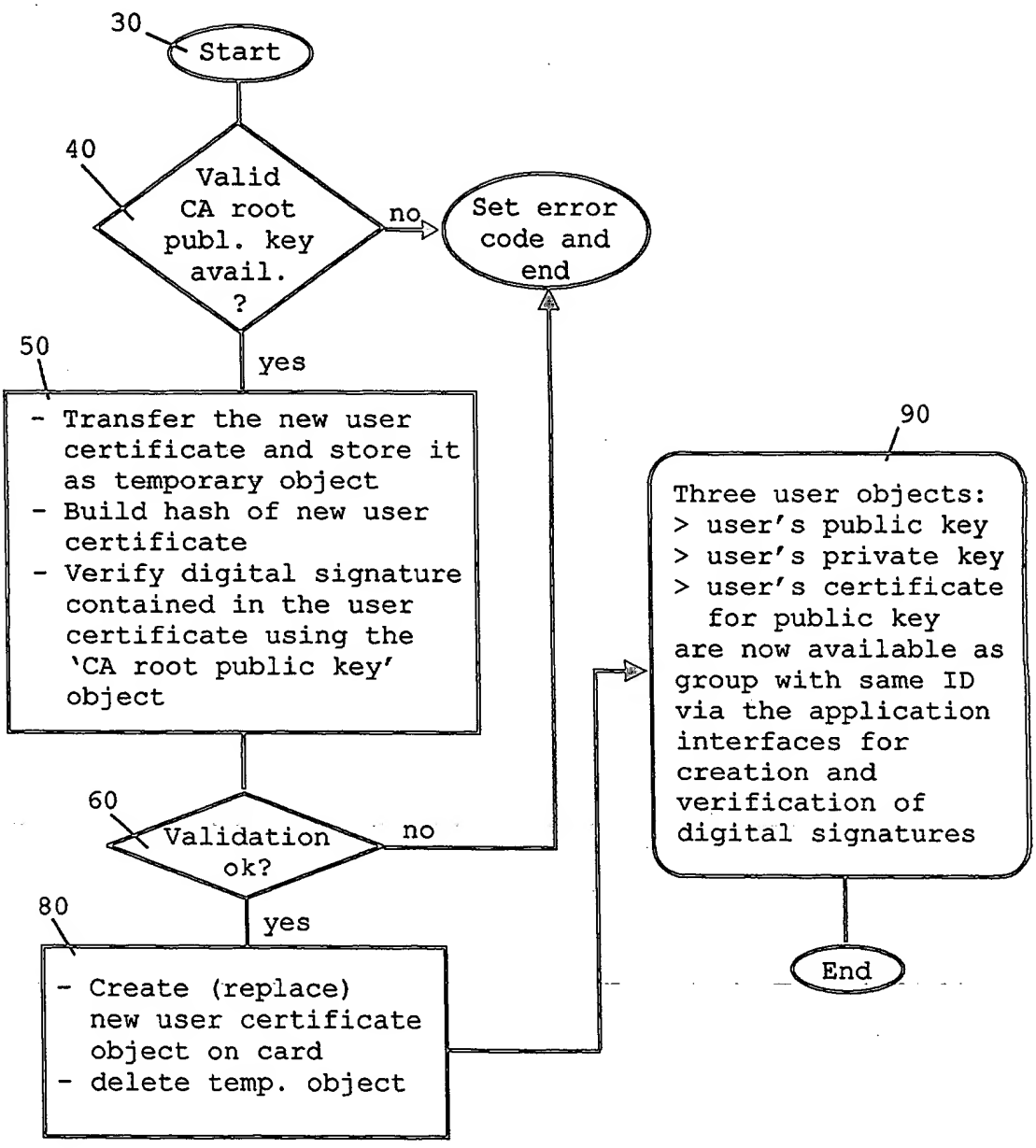
30
Start
40
Valid CA root publ. key avail. ?
no
Set error code and end
yes
50
- Transfer the new user certificate and store it as temporary object
- Build hash of new user certificate
- Verify digital signature contained in the user certificate using the 'CA root public key' object
60
Validation ok?
no
yes
80
- Create (replace) new user certificate object on card
- delete temp. object
90
Three user objects:
> user's public key
> user's private key
> user's certificate for public key
are now available as group with same ID via the application interfaces for creation and verification of digital signatures
End

FIG. 3

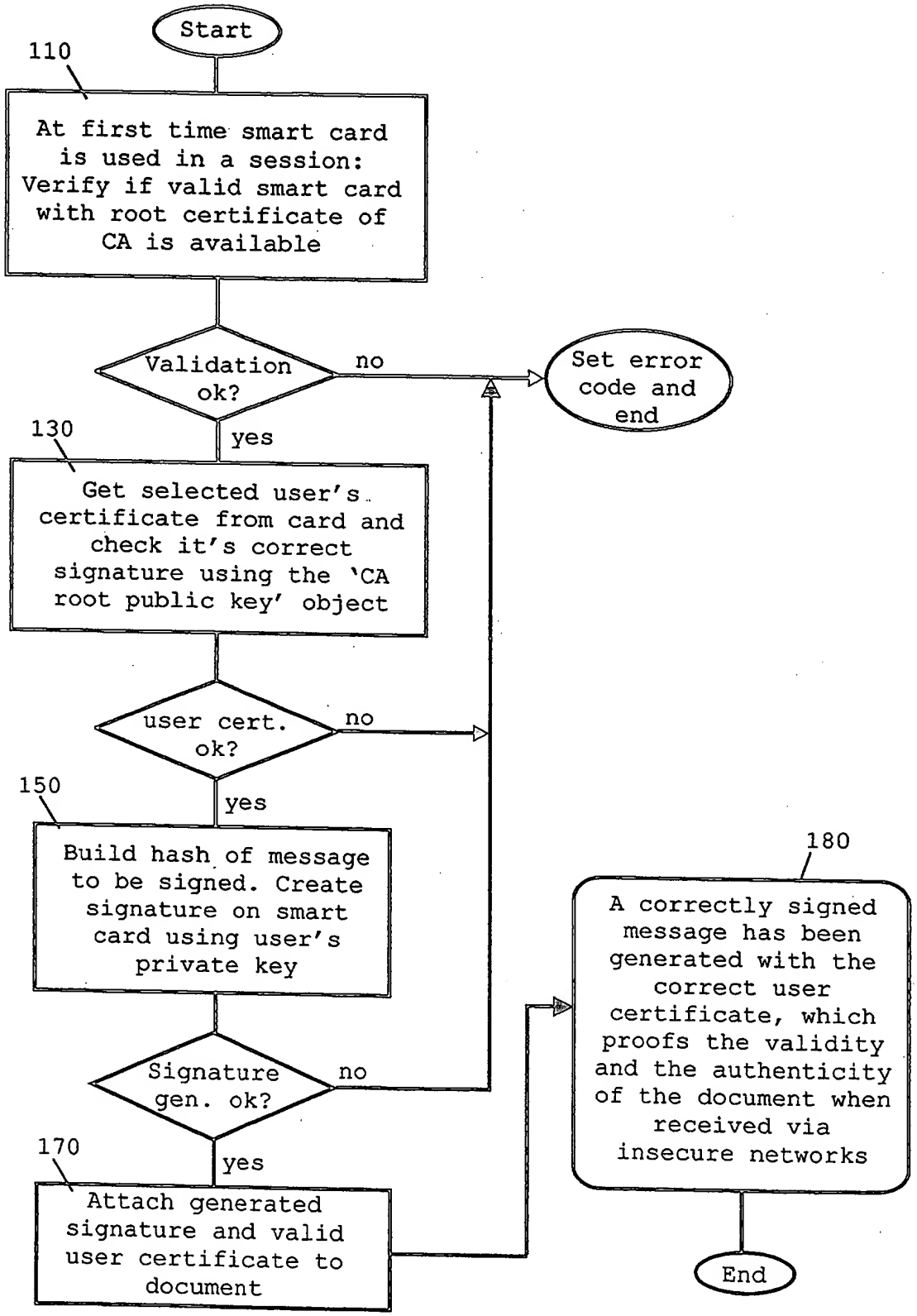
Start
110
At first time smart card is used in a session: Verify if valid smart card with root certificate of CA is available
Validation ok?
no
Set error code and end
yes
130
Get selected user's certificate from card and check it's correct signature using the 'CA root public key' object
user cert. ok?
no
yes
150
Build hash of message to be signed. Create signature on smart card using user's private key
Signature gen. ok?
no
yes
170
Attach generated signature and valid user certificate to document
180
A correctly signed message has been generated with the correct user certificate, which proofs the validity and the authenticity of the document when received via insecure networks
End

FIG. 4

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.